



# КАК НЕ СТАТЬ ЖЕРТВОЙ ВИШИНГА

**Вишинг (голосовой фишинг - voice fishing)** - один из методов мошенничества с использованием социальной инженерии. Злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предложениями выманивают у держателя платежной карты конфиденциальную информацию (ее реквизиты, номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды) или стимулируют к совершению определенных действий со своим карточным счетом/платежной картой.



Вам позвонили/прислали СМС "из банка" с неизвестного номера:

- не торопитесь следовать инструкциям;
- не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка;
- проверьте информацию, позвонив в контактный центр банка;
- незамедлительно обратитесь в правоохранительные органы.



Вам позвонили/прислали СМС с неизвестного номера с просьбой о помощи близкому человеку:

- не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей; задайте звонящему вопросы личного характера, помогающие отличить близкого вам человека от мошенника;
- под любым предложением постарайтесь прервать контакт с собеседником, позвоните родным и узнайте, все ли у них в порядке.



Вы заподозрили интернет-продавца в недобросовестности:

необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки; никогда не переводите деньги незнакомым людям в качестве предоплаты.